

Information Management Policy

Document name/title	Information Management Policy
Version number	2.0
Status (draft, published or superseded)	Published
Department/Team	Information Management and Compliance Service
Relevant or related policies/standards	IM policies and guides
Distribution (internal or external)	Internal
Author/Owner (if different name both)	Information Management and Compliance Service
Approved by	Alan McGann
Date of sign off	November 2020
Review by	31 January 2023
Security classification	Official

Contents

Introduction, purpose, and scope	3
Statutory framework.....	4
Roles and responsibilities.....	4
Managing risk to information.....	5
Protection of personal data	5
Storage of information at the ICO	5
Security of our information	6
Retention and disposal	6
Appraisal and selection for transfer to the National Archives	6
Additional policies and training	6
Monitoring and compliance	6
Version history	7

Introduction, purpose, and scope

This high-level policy sets out our commitment to following good information management practices. Our approach is guided by the section 46 Code of Practice on the Management of Records (the Code) and is based on the principles articulated in the Code.

In writing this policy, we've considered the nature of the information we hold, the work we do and the legal requirement for confidentiality imposed on the Commissioner and his staff.

Effective information management helps to ensure we have the right information at the right time to make the right decisions. We are committed to service excellence and information management is vital to the delivery of our services in an orderly, efficient, and accountable manner.

Our information is a valuable corporate asset, and our records provide evidence of what we do and why. We aim to balance our commitment to openness and transparency with our responsibilities as an effective regulator. We know what information we hold, why we hold it and we manage information according to its sensitivity. We create and manage records efficiently, make them accessible where possible, protect and store them securely and dispose of them safely at the right time.

We have the appropriate governance, organisational capacity, and technical measures in place to manage information in accordance with the Code.

By adopting this policy, we aim to ensure that information, whatever form it takes, is accurate, reliable, ordered, complete, useful, up to date and accessible whenever it is needed to:

- help us carry out our business,
- help us to make informed decisions,
- protect the rights of our employees, the public and those we regulate,
- track policy changes and development,
- make sure we comply with relevant legislation,
- provide an audit trail to meet business, regulatory and legal requirements
- make sure we have the essential tools to search, identify, locate and retrieve information,
- make sure we work effectively as a regulator and prosecuting authority and meet our lawful obligations for disclosing evidence in relation Public Inquiries or legal action,

- support continuity and consistency in management and administration,
- make sure we are open, transparent, and responsive,
- support the maintenance of our publication scheme,
- support research and development; and
- promote our achievements.

This policy together with associated guidance and procedures applies to the management of all information, in both digital and physical formats, created or received by us. It applies to all staff, contractors, consultants and third parties who are given access to our documents and information processing facilities.

Statutory framework

This policy provides a framework for meeting our information management responsibilities under relevant legislation, guidance and codes of practice including the:

- UK General Data Protection Regulation (UK GDPR)
- Data Protection Act 2018 (DPA 2018)
- Freedom of Information Act 2000
- Public Records Act 1958 (PRA 1958)
- Re-use of Public Sector Information Regulations 2015
- Section 46 Code of Practice on the management of records
- [ICO's Code of Conduct](#)

Roles and responsibilities

All staff have a responsibility to ensure we manage our information and any associated risks appropriately and in accordance with this policy and its associated guidance and procedures.

To ensure that responsibility for delivering good standards of information management practice is embedded throughout the organisation we have a [Information Risk Management Network](#) that assigns specific roles to individual staff. We provide these staff with [specific guidance](#) covering their role and their responsibilities.

In summary, the membership of the network is as follows:

- Data Protection Officer (DPO)
- Senior Information Risk Owner (SIRO)
- Information Asset Owners (IAOs)
- Information Asset Managers (IAMs)
- Local Information Management Officers (LIMOs)

- SharePoint Site Owners (SOs)

Our SIRO is our Deputy Chief Executive and Chief Operating Officer and our IAOs are our Directors. Our DPO sits on all our risk and compliance committees. Our Risk and Governance Board (RGB), chaired by the SIRO, is concerned with ensuring that risk to information is appropriately managed.

Central support to the Information Risk Management Network is provided by several teams at the ICO with responsibilities and appropriate skills to deliver the following functions: Information Management, Information Security, Risk Management, Information Access, Facilities, IT teams, legal teams, procurement, and HR.

The compliance teams also produce various policies, procedures and guidance and make them available to all staff in a central corporate repository.

A group manager heads the information management and compliance team. This team is responsible for the day-to-day management of ICO information and for producing policies, procedures and guidance.

Managing risk to information

RGB provides overview and scrutiny of information governance (IG) arrangements and considers escalated IG issues from the SIRO for decisions. RGB has a permanent IG working group tasked with developing an information risk appetite statement and maintaining an IG risk register too.

Protection of personal data

[The ICO's Data Protection Policy](#) provides a framework for ensuring that the ICO meets its obligations under the UK GDPR and the DPA 2018. It applies to all the processing of personal data carried out by the ICO including processing carried out by joint controllers, contractors, and processors.

Storage of information at the ICO

We store our information in prescribed locations, appropriate to its format, content and sensitivity. We ensure appropriate controls are in place to maintain the confidentiality, integrity and availability of our information.

We have a [storage policy](#) in addition to procedures and guidance to support staff to choose the right place to store information.

Security of our information

We ensure the security of our information via the implementation of a number of policies, procedures and guidance. Our [Information Security Policy](#) supported by our [Information Classification Policy](#) ensures that information within our care receives an appropriate level of protection including access and permission control. Our staff use our systems in line with our [Acceptable Use Policy](#).

Retention and disposal

Our [Retention and Disposal Policy](#) outlines our approach to managing the retention and secure disposal of our information. It provides for a consistent approach and applies to all physical and digital information, regardless of storage location.

Our retention periods are driven by legislation or business need. If there is no legally defined retention period for corporate information, it is the responsibility of the relevant IAO (with input from the Information Management & Compliance team) to determine an appropriate retention period.

Appraisal and selection for transfer to the National Archives

We follow our [appraisal and selection methodology](#). The methodology describes how the ICO will meet its statutory obligation as a public record body under the terms of the PRA 1958. The methodology is supported by TNA training and guidance and ICO guidance.

Additional policies and training

This policy is supported by additional Information Management policies and guides that provide more detailed and subject-specific information to further its objectives. It is also supported by training e.g. the ICO's Information Governance training.

Monitoring and compliance

Ongoing monitoring of compliance with this policy and its supporting policies, guidance and procedures will be undertaken on a regular basis by the Information Management Service and those with assigned responsibilities under the [Information Risk Management Network](#). Monitoring compliance will also be supported by internal checks from the risk and compliance manager and external audits as appropriate.

Version history

Version	Changes made	Date	Made By
0.1	First Draft	20/11/2020	Ben Cudbertson
0.2	First Draft	23/11/2020	Iman El Mehdawy
1.0	Published	24/11/2020	Ben Cudbertson
2.0	Major revision	06/06/2022	Iman El Mehdawy